BUNDESREPUBLIK DEUTSCHLAND

CERTIFIED COPY OF
PRIORITY DOCUMENT

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	100 02 183.2
Anmeldetag:	19. Januar 2000
Anmelder/Inhaber:	Philips Corporate Intellectual Property GmbH, Hamburg/DE
Bezeichnung:	Drahtloses Netzwerk mit einer Schlüsseländerungsprozedur
IPC:	H 04 Q, H 04 L, H 04 B

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 9. August 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Seiler

A 9161
06/00
EDV-L

ZUSAMMENFASSUNG

Drahtloses Netzwerk mit einer Schlüsseländerungsprozedur

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals, die zur Verschlüsselung bestimmter zu übertragener Daten und zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten dienen. Zu Beginn einer Schlüsseländerungsprozedur wird die Übertragung von Dateneinheiten angehalten. Die Funknetzwerk-Steuerung startet nach dem Austausch von Meldungen über den Zeitpunkt der Gültigkeit des neuen Schlüssels eine Prozedur zur Ermittlung, ob auch wenigstens ein Terminal den neuen Schlüssel verwendet. Nach der Prozedur wird die Übertragung von Dateneinheiten in Abhängigkeit von dem Prozedurergebnis mit dem neuen oder alten Schlüssel wieder aufgenommen.

Fig. 5

19.01.00

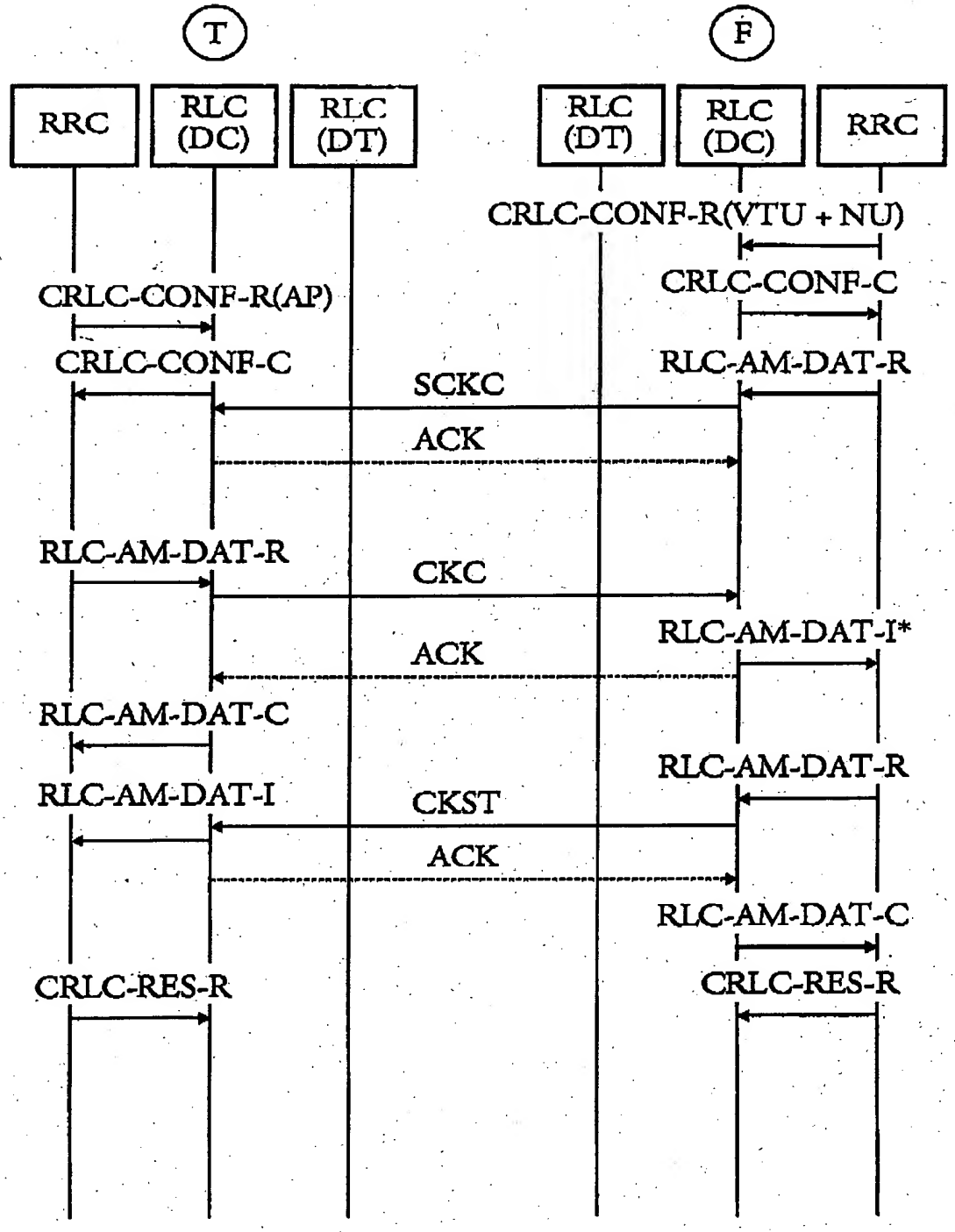

FIG. 5

PHDE000011

BESCHREIBUNG

Drahtloses Netzwerk mit einer Schlüsseländerungsprozedur

Die Erfindung bezieht sich auf ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals,

- die zur Verschlüsselung bestimmter zu übertragener Daten,
- die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten und
- zu Beginn der Schlüsseländerung zum Anhalten der Übertragung von Dateneinheiten vorgesehen sind.

Aus dem Buch „The GSM System for Mobile Communications" von Michel Mouly und Marie-Bernadette Pautet, Verlag Cell & Sys, 1992, Seiten 391 bis 395, ist bekannt, dass Daten zwischen einer Basisstation und einem Terminal verschlüsselt übertragen werden. Der für die Übertragung benötigte Schlüssel wird in bestimmten Zeitabständen verändert. Hierfür ist eine Prozedur in drei Schritten vorgesehen.

Der Erfindung liegt die Aufgabe zugrunde, ein drahtloses Netzwerk zu schaffen, das eine andere Prozedur zur Änderung eines Schlüssels angibt.

Die Aufgabe wird durch ein drahtloses Netzwerk der eingangs genannten Art dadurch gelöst,
dass die Funknetzwerk-Steuerung nach dem Austausch von Meldungen über den Zeitpunkt der Gültigkeit des neuen Schlüssels zur Ermittlung vorgesehen ist, ob auch wenigstens ein Terminal den neuen Schlüssel verwendet, und nach der Überprüfung zum Aufnehmen der Übertragung von Dateneinheiten in Abhängigkeit von dem Überprüfungsergebnis mit dem neuen oder alten Schlüssel vorgesehen ist.

Unter dem erfindungsgemäßen drahtlosen Netzwerk ist ein Netzwerk mit mehreren Funkzellen zu verstehen, in denen jeweils eine Basisstation und mehrere Terminals Steuer- und Nutzdaten drahtlos übertragen. Eine drahtlose Übertragung dient zur Übertragung

von Informationen z.B. über Funk-, Ultraschall- oder Infrarotwege.

Erfindungsgemäß wird die Übertragung von Dateneinheiten zwischen wenigstens einem Terminal und der Funknetzwerk-Steuerung angehalten und dann überprüft ob ein Terminal und die Funknetzwerk-Steuerung denselben Schlüssel benutzen. Ist dies der Fall wird die Übertragung von Dateneinheiten mit dem neuen Schlüssel wieder aufgenommen. Im anderen Fall wird die Übertragung von Dateneinheiten mit dem alten Schlüssel fortgesetzt.

Ausführungsbeispiele der Erfindung werden nachstehend anhand der Fig. näher erläutert. Es zeigen:

Fig. 1	ein drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren Terminals,
Fig. 2	ein Schichtenmodell zur Erläuterung verschiedener Funktionen eines Terminals oder einer Funknetzwerk-Steuerung,
Fig. 3	ein Blockschaltbild zur Erläuterung des Verschlüsselungsmechanismus in einem Terminal oder einer Funknetzwerk-Steuerung und
Fig. 4 bis 6	Ablauf verschiedener Meldungen bei einer Schlüsseländerungsprozedur.

In Fig. 1 ist ein drahtloses Netzwerk, z.B. Funknetzwerk, mit einer Funknetzwerk-Steuerung (Radio Network Controller = RNC) 1 und mehreren Terminals 2 bis 9 dargestellt. Die Funknetzwerk-Steuerung 1 ist für Steuerung aller am Funkverkehr beteiligten Komponenten verantwortlich, wie z.B. der Terminals 2 bis 9. Ein Steuer- und Nutzdatenaustausch findet zumindest zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 statt. Die Funknetzwerk-Steuerung 1 baut jeweils eine Verbindung zur Übertragung von Nutzdaten auf.

In der Regel sind die Terminals 2 bis 9 Mobilstationen und die Funknetzwerk-Steuerung 1 ist fest installiert. Eine Funknetzwerk-Steuerung 1 kann gegebenenfalls aber auch beweglich bzw. mobil sein.

In dem drahtlosen Netzwerk werden beispielsweise Funksignale nach dem FDMA-, TDMA- oder CDMA-Verfahren (FDMA = frequency division multiplex access, TDMA = time division multiplex access, CDMA = code division multiplex access) oder nach einer Kombination der Verfahren übertragen.

Beim CDMA-Verfahren, das ein spezielles Code-Spreiz-Verfahren (code spreading) ist, wird eine von einem Anwender stammende Binärinformation (Datensignal) mit jeweils einer unterschiedlichen Codesequenz moduliert. Eine solche Codesequenz besteht aus einem pseudo-zufälligen Rechtecksignal (pseudo noise code), dessen Rate, auch Chiprate genannt, in der Regel wesentlich höher als die der Binärinformation ist. Die Dauer eines Rechteckimpulses des pseudo-zufälligen Rechtecksignals wird als Chipintervall T_C bezeichnet. $1/T_C$ ist die Chiprate. Die Multiplikation bzw. Modulation des Datensignals mit dem pseudo-zufälligen Rechtecksignal hat eine Spreizung des Spektrums um den Spreizungsfaktor $N_C = T/T_C$ zur Folge, wobei T die Dauer eines Rechteckimpulses des Datensignals ist.

Nutzdaten und Steuerdaten zwischen wenigstens einem Terminal (2 bis 9) und der Funknetzwerk-Steuerung 1 werden über von der Funknetzwerk-Steuerung 1 vorgegebene Kanäle übertragen. Ein Kanal ist durch einen Frequenzbereich, einen Zeitbereich und z.B. beim CDMA-Verfahren durch einen Spreizungscode bestimmt. Die Funkverbindung von der Funknetzwerk-Steuerung 1 zu den Terminals 2 bis 9 wird als Downlink und von den Terminals zur Basisstation als Uplink bezeichnet. Somit werden über Downlink-Kanäle Daten von der Basisstation zu den Terminals und über Uplink-Kanäle Daten von Terminals zur Basisstation gesendet.

Beispielsweise kann ein Downlink-Steuerkanal vorgesehen sein, der benutzt wird, um von der Funknetzwerk-Steuerung 1 Steuerdaten vor einem Verbindungsaufbau an alle Terminals 2 bis 9 zu verteilen. Ein solcher Kanal wird als Downlink-Verteil-Steuerkanal (broadcast control channel) bezeichnet. Zur Übertragung von Steuerdaten vor einem Verbindungsaufbau von einem Terminal 2 bis 9 zur Funknetzwerk-Steuerung 1 kann beispielsweise ein von der Funknetzwerk-Steuerung 1 zugewiesener Uplink-Steuerkanal verwendet werden, auf den aber auch andere Terminals 2 bis 9 zugreifen können. Ein

Uplink-Kanal, der von mehreren oder allen Terminals 2 bis 9 benutzt werden kann, wird als gemeinsamer Uplink-Kanal (common uplink channel) bezeichnet. Nach einem Verbindungsaufbau z.B. zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1 werden Nutzdaten über einen Downlink- und ein Uplink-Nutzkanal übertragen. Kanäle, die nur zwischen einem Sender und einem Empfänger aufgebaut werden, werden als dedizierte Kanäle bezeichnet. In der Regel ist ein Nutzkanal ein dedizierter Kanal, der von einem dedizierten Steuerkanal zur Übertragung von verbindungsspezifischen Steuerdaten begleitet werden kann.

Damit Nutzdaten zwischen der Funknetzwerk-Steuerung 1 und einem Terminal ausgetauscht werden können, ist es erforderlich, dass ein Terminal 2 bis 9 mit der Funknetzwerk-Steuerung 1 synchronisiert wird. Beispielsweise ist aus dem GSM-System (GSM = Global System for Mobile communication) bekannt, in welchem eine Kombination aus FDMA- und TDMA-Verfahren benutzt wird, dass nach der Bestimmung eines geeigneten Frequenzbereichs anhand vorgegebener Parameter die zeitliche Position eines Rahmens bestimmt wird (Rahmensynchronisation), mit dessen Hilfe die zeitliche Abfolge zur Übertragung von Daten erfolgt. Ein solcher Rahmen ist immer für die Datensynchronisation von Terminals und Basisstation bei TDMA-, FDMA- und CDMA-Verfahren notwendig. Ein solcher Rahmen kann verschiedene Unter- oder Subrahmen enthalten oder mit mehreren anderen aufeinanderfolgenden Rahmen einen Superrahmen bilden. Aus Vereinfachungsgründen wird im folgenden von einem Rahmen ausgegangen, der als Referenzrahmen bezeichnet wird.

Die Steuer- und Nutzdatenaustausch über die Funkschnittstelle zwischen der Funknetzwerk-Steuerung 1 und den Terminals 2 bis 9 kann mit dem in Fig. 2 dargestellten, beispielhaften Schichtenmodell oder Protokollarchitektur (vgl. z.B. 3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) RAN; Working Group 2 (WG2); Radio Interface Protocol Architecture; TS 25.301 V3.2.0 (1999-10)) erläutert werden. Das Schichtenmodell besteht aus drei Protokollschichten: der physikalischen Schicht PHY, der Datenverbindungsschicht mit den Unterschichten MAC und RLC (in Fig. 2 sind mehrere Ausprägungen der Unterschicht RLC dargestellt) und der Schicht RRC. Die Unterschicht MAC ist für die Medienzugriffssteuerung (Medium Access Control), die Unterschicht

RLC für die Funkverbindungssteuerung (Radio Link Control) und die Schicht RRC für die Funkverwaltungssteuerung (Radio Resource Control) zuständig. Die Schicht RRC ist für die Signalisierung zwischen den Terminals 2 bis 9 und der Funknetzwerk-Steuerung 1 verantwortlich. Die Unterschicht RLC dient zur Steuerung einer Funkverbindung zwischen einem Terminal 2 bis 9 und der Funknetzwerk-Steuerung 1. Die Schicht RRC steuert die Schichten MAC und PHY über Steuerungsverbindungen 10 und 11. Hiermit kann die Schicht RRC die Konfiguration der Schichten MAC und PHY steuern. Die physikalische Schicht PHY bietet der MAC-Schicht Transportverbindungen 12 an. Die MAC-Schicht stellt der RLC-Schicht logische Verbindungen 13 zur Verfügung. Die RLC-Schicht ist über Zugangspunkte 14 von Applikationen erreichbar.

Bei einem solchen drahtlosen Netzwerk werden die Daten aus Sicherheits- und Vertraulichkeitsgründen verschlüsselt über die Funkschnittstelle übertragen, um eine Abhören der Daten zu verhindern. Die Verschlüsselung wird in der Datenverbindungsschicht (z. B. in der RLC- oder MAC-Schicht) durchgeführt. Wie Fig. 3 zeigt, werden die Daten D über eine Exklusiv-Oder-Funktion (XOR) mit einer Verschlüsselungsmaske M verknüpft, so dass sich ein verschlüsselter Datenstrom C_D ergibt. Die Verschlüsselungsmaske M wird in einer Verschlüsselungs-Funktion 16 gebildet, die nach einem Verschlüsselungs-Algorithmus arbeitet und als Eingangswerte den Schlüssel CK und andere hier nicht näher dargestellte Parameter P erhält.

Der Schlüssel muss sowohl der Funknetzwerk-Steuerung 1 als auch den Terminals 2 bis 9 bekannt sein. Dieser Schlüssel wird zu bestimmten Zeitpunkten (z.B. alle 2 Stunden) mit einer speziellen Prozedur CKC (cipher key change) geändert, die als Schlüsseländerungs-Prozedur bezeichnet wird. Bei dieser Prozedur werden Meldungen zwischen den Schichten RLC und RRC übertragen. In der Schicht RLC werden dabei noch Meldungen zwischen eigenen Instanzen RLC(DC) und RLC(DT) ausgetauscht. Die Instanz RLC(DT) ist für die Steuerung von dedizierten Nutzkanälen (dedicated traffic channel = DTCH) und die Instanz RLC(DC) für die Steuerung von dedizierten Steuerungskanälen (dedicated control channel = DCCH) zuständig.

Mit der Prozedur CKC wird von der Funknetzwerk-Steuerung 1 den Terminals 2 bis 9 die

Gültigkeit eines neuen Schlüssels mitgeteilt. Dieser neue Schlüssel ist sowohl der Funknetzwerk-Steuerung 1 als auch den Terminals 2 bis 9 bekannt. Die Fig. 4 bis 6 zeigen verschiedene Meldungen, die zwischen den Schichten RRC und RLC eines Terminals (linke Seite einer Fig. 4 bis 6, mit „T" angegeben) und der Funknetzwerk-Steuerung 1 (rechte Seite einer Fig. 4 bis 6, mit „F" angegeben) gesendet werden. Die im folgende zu beschreibende Fig. 4 stellt den Prolog der Schlüsseländerungsprozedur CKC dar. Diese Prozedur CKC wird durch die lokale Meldung CRLC-S-R(ND) von der Schicht RRC der Seite F angestoßen. Mit dieser lokalen Meldung wird der Instanz RLC(DC) mitgeteilt, dass die Übertragung von Dateneinheiten in Meldungen angehalten werden soll, sofern eine Folgenummer SN einer Dateneinheit (Jede Dateneinheit wird mit einer Folgenummer markiert) die Bedingung SN ≥ VTD + ND erfüllt. Dabei bedeutet der Parameter ND der lokalen Meldung CRLC-S-R(ND) eine Anzahl von noch zu übertragenden Dateneinheiten, und VTD ist die in RLC(DC) bekannte Folgenummer der nächsten erstmals zu sendenden Dateneinheit. Mit der lokalen Meldung CRLC-S-C(VTD) bestätigt die Instanz RLC(DC) der Seite F den Empfang der Folgenummer ND und gibt der Schicht die Nummer VTD bekannt. Anschließend teilt die Schicht RRC der Seite F der Instanz RLC(DC) über die lokale Meldung CRLC-CONF-R(CKN) den neuen zu verwendenden Schlüssel CKN mit. Diese Meldung wird von RLC(DC) der Seite F mit der lokalen Meldung CRLC-CONF-C bestätigt.

Nachdem die Schicht RRC der Instanz RLC(DC) die lokale Meldung RLC-AM-DAT-R geliefert hat, sendet die Instanz RLC(DC) der Seite F die Meldung SEC-MO-COM(VTD, ND) an die Instanz RLC(DC) der Seite T (Terminal). Diese Meldung stellt einen Befehl im Sicherheitsmode (security mode command) dar und wird mit dem alten, bisher gültigen Schlüssel verschlüsselt. In der Meldung ist eine Dateneinheit mit den Nummern VTD und ND enthalten. Nach Empfang dieser Meldung zeigt die Instanz RLC(DC) der Schicht RRC der Seite T über die lokale Meldung RLC-AM-DAT-I an, dass die Meldung mit der Angabe angekommen ist, ab wann der neue Schlüssel gelten soll. Dieser neue Schlüssel gilt für das Entschlüsseln nämlich nach der Folgenummer VTD + ND einer Dateneinheit. Der Empfang der Meldung SEC-MO-COM(VTD, ND) in der Instanz RLC(DC) der Seite T wird über einen Befehl ACK der Instanz RLC(DC) der Seite F und weiter der Schicht RRC über die lokale Meldung RLC-AM-DAT-C bestätigt.

Damit ist der Funknetzwerk-Steuerung 1 bekannt, dass das Terminal über den Beginn der Schlüsseländerungsprozedur informiert ist und den neuen Schlüssel zur Entschlüsselung von Dateneinheiten verwendet, deren Folgenummer SN die Bedingung SN ≥ VTD + ND erfüllt.

Von der Seite T (Terminal) ausgehend wird ein ähnlicher Meldungaustausch zwischen den betroffenen Schichten durchgeführt. Eine lokale Meldung CRLC-S-R(NU) von der Schicht RRC der Seite T startet den von der Seite T ausgehenden Meldungsaustausch. Mit dieser Meldung wird die Übertragung von Dateneinheiten angehalten, deren Folgenummer SN die Bedingung SN ≥ VTU + NU erfüllt. Der Instanz RLC(DC) wird die Anzahl NU von noch zu übertragenen Dateneinheiten mitgeteilt. Mit der lokalen Meldung CRLC-S-C(VTU) bestätigt die Instanz RLC(DC) der Seite T den Empfang der Nummer NU und gibt der Schicht die Nummer VTU an. Diese Nummer VTU gibt die Folgenummer SN der Dateneinheit an, die nach Empfang der lokalen Meldung CRLC-S-C(VTU) erstmals (im Uplink) gesendet wird (also keine wiederholte Übertragung). Anschließend teilt die Schicht RRC der Seite T der Instanz RLC(DC) einen Schlüsseländerungs-Wunsch über die lokale Meldung CRLC-CONF-R(CKN) mit. Diese Meldung wird von RLC(DC) der Seite T mit der lokalen Meldung CRLC-CONF-C bestätigt.

Mit der lokalen Meldung RLC-AM-DAT-R von der Schicht RRC der Seite T an die Instanz RLC(DC) wird der Prozedurteil gestartet, mit welcher angegeben wird, ab wann der neue Schlüssel für die Seite T gilt. Nach dem Empfang der lokalen Meldung RLC-AM-DAT-R, sendet die Instanz RLC(DC) der Seite T (Terminal) die Meldung SEC-MO-CMPL(VTU, NU) an die Instanz RLC(DC) der Seite F (Funknetzwerk-Steuerung). Diese Meldung stellt einen Befehl im Sicherheitsmode (security mode complete) dar und wird mit dem alten, bisher gültigen Schlüssel verschlüsselt. In der Meldung ist eine Dateneinheit mit den Nummern VTU und NU enthalten. Nach Empfang dieser Meldung zeigt die Instanz RLC(DC) der Schicht RRC der Seite F über die lokale Meldung RLC-AM-DAT-I an, dass die Meldung mit der Angabe angekommen ist, ab wann der neue Schlüssel zum Entschlüsseln in der Funknetzwerk-Steuerung 1 gelten soll. Dieser neue Schlüssel gilt nämlich nach der Folgenummer VTU + NU einer Dateneinheit. Der Empfang der

Meldung SEC-MO-CMPL(VTU, NU) in der Instanz RLC(DC) der Seite F wird über einen Befehl ACK der Instanz RLC(DC) der Seite F und weiter der Schicht RRC über die lokale Meldung RLC-AM-DAT-C bestätigt. Damit ist dem Terminal bekannt, dass der Funknetzwerk-Steuerung 1 bekannt ist, dass das Terminal den neuen Schlüssel zum Verschlüsseln von Dateneinheiten eigener Meldungen ab der Folgenummer VTU + NU verwendet.

Die Fig. 5 zeigt einen weiteren auf den Prolog folgenden Teil der Prozedur, der als erster Prüfteil bezeichnet wird. Hierbei werden mit dem neuen Schlüssel verschlüsselte Dateneinheiten in Meldungen von den beiden Seiten T und F korrekt verschlüsselt und erkannt. Der erste Prüfteil startet mit der lokalen Meldung CRLC-CONF-R(VTU + NU), die auf der Seite F von der Schicht RRC zur Instanz RLC(DC) transferiert wird. Damit wird der Instanz RLC(DC) mitgeteilt, dass alle vom Terminal empfangenen Meldungen mit dem neuen Schlüssel entschlüsselt werden sollen, wenn für die Folgenummer SN der nächsten Dateneinheit die Bedingung SN ≥ VTU + NU oder SN = VR gilt, wobei VR die nächste erwartete, erstmals zu sendende Dateneinheit darstellt. Die Instanz RLC(DC) bestätigt den Empfang der lokalen Meldung CRLC-CONF-R(VTU + NU) durch das Versenden der lokalen Meldung CRLC-CONF-C an die Schicht RRC. Auf der Seite T wird mit dem Transfer der lokalen Meldung CRLC-CONF-R(APNK) von der Schicht RRC zur Instanz RLC(DC) der Instanz RLC(DC) mitgeteilt, dass nach dieser Meldung die nächsten zur Seite F (Funknetzwerk-Steuerung 1) zu übertragenden Dateneinheiten mit dem neuen Schlüssel verschlüsselt werden. Empfangene Meldungen der Seite F müssen jedoch noch mit dem alten Schlüssel entschlüsselt werden. Die Instanz RLC(DC) bestätigt der Schicht RRC auf der Seite T den Empfang der lokalen Meldung CRLC-CONF-R(APNK) mit der lokalen Meldung CRLC-CONF-C.

Mit dem folgenden Meldungsablauf wird geprüft, ob beide Seiten T und F denselben neuen Schlüssel verwenden. Dieser Meldungsablauf wird von der Schicht RRC der Seite F mit der lokalen Meldung RLC-AM-DAT-R an die Instanz RLC(DC) gestartet. Hiermit wird die Instanz RLC(DC) der Seite F aufgefordert, eine mit dem alten Schlüssel verschlüsselte Meldung SCKC an die Instanz RLC(DC) der Seite T zu senden. Nach Empfang dieser Meldung SCKC sendet die Instanz RLC(DC) der Seite T eine

Empfangsbestätigung ACK an die Instanz RLC(DC) der Seite F. Die Schicht RRC der Seite T übergibt in der lokalen Meldung RLC-AM-DAT-R der Instanz RLC(DC) der Seite T eine Nachricht N(CKC), welche die Instanz RLC(DC) der Seite T in eine oder mehrere Dateneinheiten zerlegt. Die Instanz RLC(DC) der Seite T verschlüsselt diese Dateneinheiten mit dem neuen Schlüssel und sendet sie (Meldung CKC in Fig. 5) an die Instanz RLC(DC) der Seite F. Die Instanz RLC(DC) der Seite F entschlüsselt alle empfangenen Dateneinheiten der Meldung CKC mit dem neuen Schlüssel, baut die Nachricht N(CKC) aus den in der Meldung CKC gesendeten Dateneinheiten zusammen und übergibt diese Nachricht N(CKC) in der lokalen Meldung RLC-AM-DAT-I* an die Schicht RRC der Seite F. Die lokale Meldung RLC-AM-DAT-I* wird nur für die Nachricht N(CKC) verwendet, deren erste Dateneinheit nach Empfang der lokalen Meldung CRLC-CONF-R(VTU + NU) die Folgenummer SN = VR hatte (diese ist gerade die Meldung CKC). Dadurch weiß die Schicht RRC der Seite F, dass sie die Nachricht N(CKC) von der Instanz RLC(DC) entgegennimmt.

Wurde von der Seite T der richtige neue Schlüssel verwendet, so erhält die Schicht RRC der Seite F in der lokalen Meldung RLC-AM-DAT-I* die erwartete Nachricht N(CKC). Wurde von der Seite T ein falscher neuer Schlüssel verwendet, so erhält die Schicht RRC der Seite F in der lokalen Meldung RLC-AM-DAT-I* eine sinnlose oder unbekannte Meldung. Daraus schließt die Schicht RRC der Seite F, dass die Seite T einen falschen Schlüssel verwendet hat, d.h. die unbekannte Meldung wird in diesem speziellen Fall nicht ignoriert.

Nach Empfang der Meldung CKC bestätigt die Instanz RLC(DC) der Seite F der Instanz RLC(DC) der Seite T den Empfang der Meldung CKC durch den Befehl ACK. Der Empfang wird von der Instanz RLC(DC) der Seite T durch die lokale Meldung RLC-AM-DAT-C an die Schicht RRC weitergereicht.

Nach Empfang der in der Meldung RLC-AM-DAT-I* enthaltenen Nachricht sendet die Schicht RRC der Seite F die Nachricht N(CKST), die einen Hinweis darüber enthält, ob die Seite T den richtigen oder einen falschen neuen Schlüssel verwendet (CKST = Cipher Key Status) hat, an die Schicht RRC von T. Dieses geschieht wieder dadurch, dass die

Schicht RRC der Seite F in der lokalen Meldung RLC-AM-DAT-R diese Nachricht N(CKST) an die Instanz RLC(DC) der Seite F gibt, die diese Nachricht in eine oder mehrere Dateneinheiten zerlegt und mit dem alten Schlüssel verschlüsselt an die Instanz RLC(DC) der Seite T mit der Meldung CKST sendet. Die Instanz RLC(DC) der Seite T bestätigt mit der Meldung ACK den Erhalt dieser Dateneinheiten, entschlüsselt sie mit dem alten Schlüssel und baut die Nachricht N(CKST) wieder zusammen. Diese Nachricht N(CKST) wird in einer lokalen Meldung RLC-AM-DAT-I an die Schicht RRC der Seite T weitergereicht.

Wird auf der Seite T der richtige neue Schlüssel verwendet, so instruiert die Schicht RRC der Seite F die Instanz RLC(DC) mit der lokalen Meldung CRLC-RES-R, die Übertagung von Dateneinheiten unter Verwendung des neuen Schlüssels wieder aufzunehmen. Das Entschlüsseln auf der Seite F erfolgt mit dem neuen Schlüssel, wenn für die Folgenummer SN der empfangenen Dateneinheit gilt SN ≥ VTU + NU.

Enthält die Meldung CKST die Bestätigung, dass der von der Seite T verwendete neue Schlüssel korrekt ist, so instruiert die Schicht RRC der Seite T ihre Instanz RLC(DC) mit der lokalen Meldung CRLC-RES-R, die Übertagung von Dateneinheiten unter Verwendung des neuen Schlüssels wieder aufzunehmen. Das Entschlüsseln auf der Seite T erfolgt mit dem neuen Schlüssel, wenn für die Folgenummer SN der empfangenen Dateneinheit gilt SN ≥ VTD + ND (Fig. 5).

Wird auf der Seite T ein falscher neuer Schlüssel verwendet (vgl. Fig. 6), so instruiert die Schicht RRC der Seite F die Instanz RLC(DC) der Seite F mit der lokalen Meldung CRLC-CONF-R darüber, dass die Umstellung auf den neuen Schlüssel für das Entschlüsseln bei Erfüllung der Bedingung SN ≥ VTU + NU wieder rückgängig gemacht wird. Für das Verschlüsseln von Dateneinheiten, deren Übertragung noch angehalten ist, wird ebenfalls wieder der alte Schlüssel verwendet Die lokale Meldung CRLC-CONF-R wird durch die lokale Meldung CRLC-CONF-C von der Instanz RLC(DC) quittiert. Mit einer lokalen Meldung CRLC-RES-R teilt die Schicht RRC der Seite F der Instanz RLC(DC) mit, die Übertagung von Dateneinheiten (mit dem alten Schlüssel) wieder aufzunehmen.

Enthält die Meldung CKST den Hinweis, dass der von Seite T verwendete neue Schlüssel nicht der richtige ist, so instruiert die Schicht RRC der Seite T die Instanz RLC(DC) mit einer lokalen Meldung CRLC-CONF-R, welche mit einer Meldung CRLC-CONF-C quittiert wird, dass die Umstellung auf den neuen Schlüssel für das Entschlüsseln bei Erfüllung der Bedingung SN>=VTD+ND wieder rückgängig gemacht wird. Für das Verschlüsseln von Dateneinheiten, deren Übertragung noch angehalten ist, wird ebenfalls der alte Schlüssel verwendet. Mit einer lokalen Meldung CRLC-RES-R teilt die Schicht RRC der Seite F der Instanz RLC(DC) mit, die Übertagung von Dateneinheiten (mit dem alten Schlüssel) wieder aufzunehmen.

PATENTANSPRÜCHE

1. Drahtloses Netzwerk mit einer Funknetzwerk-Steuerung und mehreren zugeordneten Terminals,

- die zur Verschlüsselung bestimmter zu übertragener Daten,
- die zur Veränderung des für die Verschlüsselung notwendigen jeweiligen Schlüssels zu bestimmten Zeitpunkten und
- zu Beginn der Schlüsseländerung zum Anhalten der Übertragung von Dateneinheiten vorgesehen sind,

dadurch gekennzeichnet,

dass die Funknetzwerk-Steuerung nach dem Austausch von Meldungen über den Zeitpunkt der Gültigkeit des neuen Schlüssels zur Ermittlung vorgesehen ist, ob auch wenigstens ein Terminal den neuen Schlüssel verwendet, und nach der Überprüfung zum Aufnehmen der Übertragung von Dateneinheiten in Abhängigkeit von dem Überprüfungsergebnis mit dem neuen oder alten Schlüssel vorgesehen ist.

19.01.00

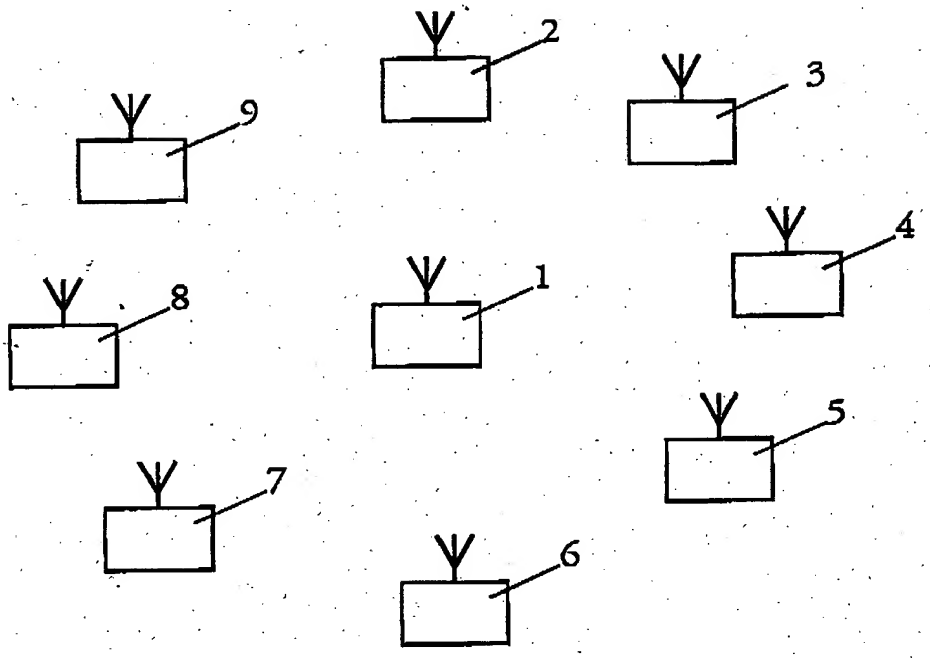

FIG. 1

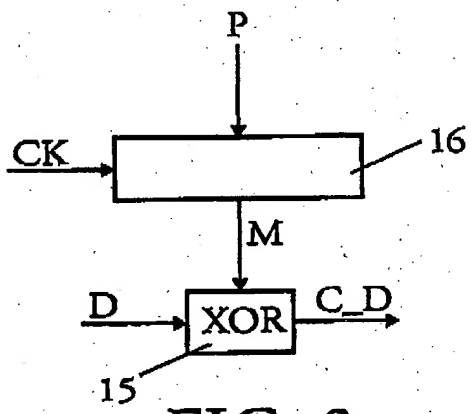

FIG. 3

19.01.00

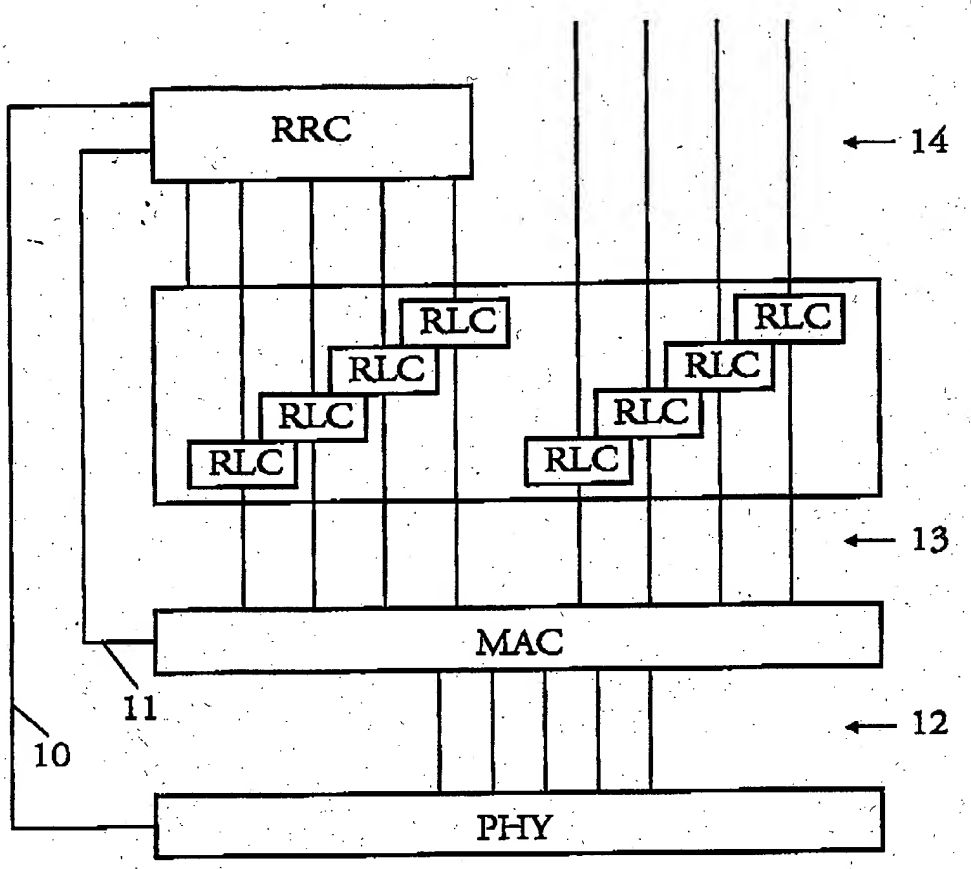

FIG. 2

2-V-PHDE000011

19.01.00

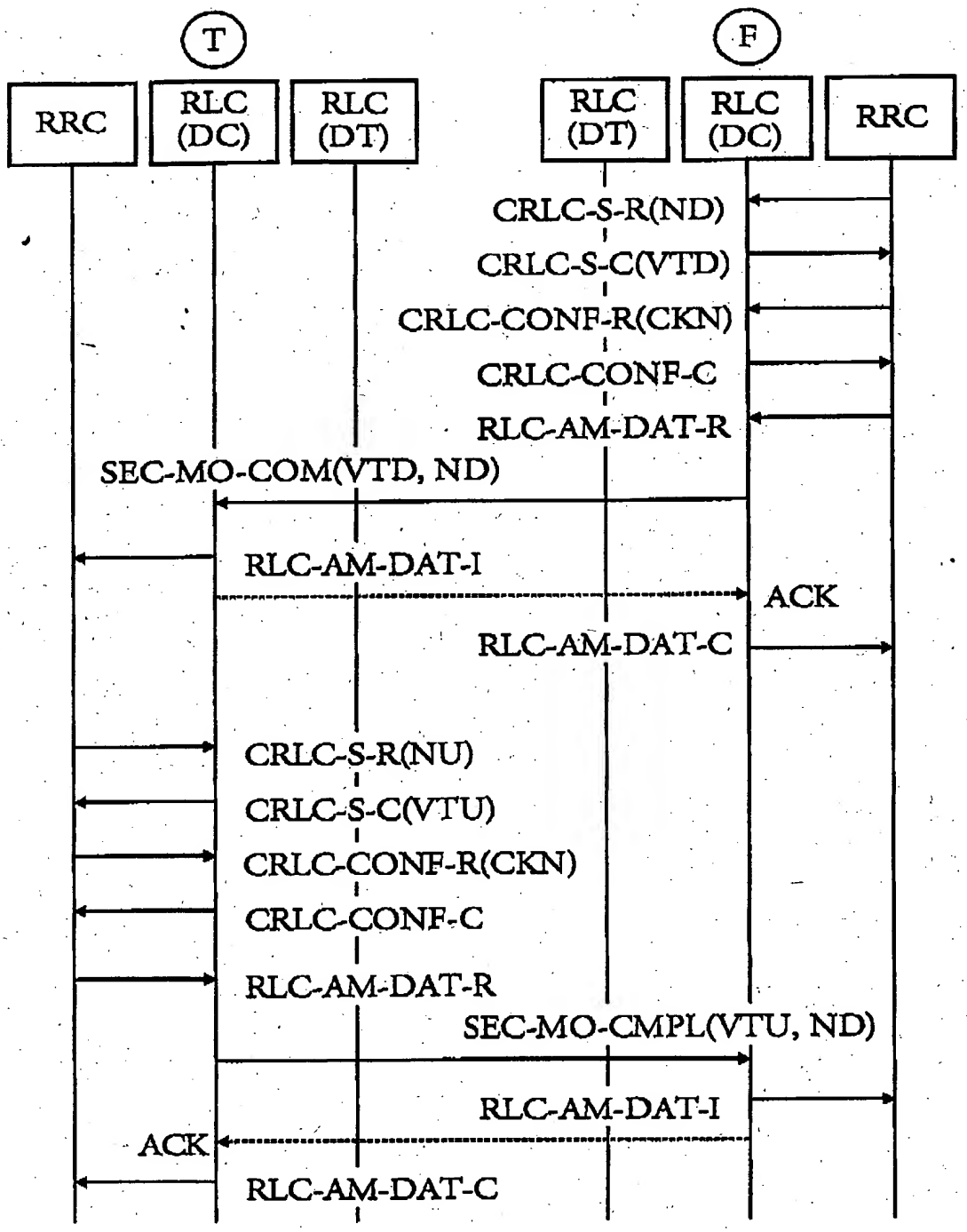

FIG. 4

3-V-PHDE000011

19.01.00

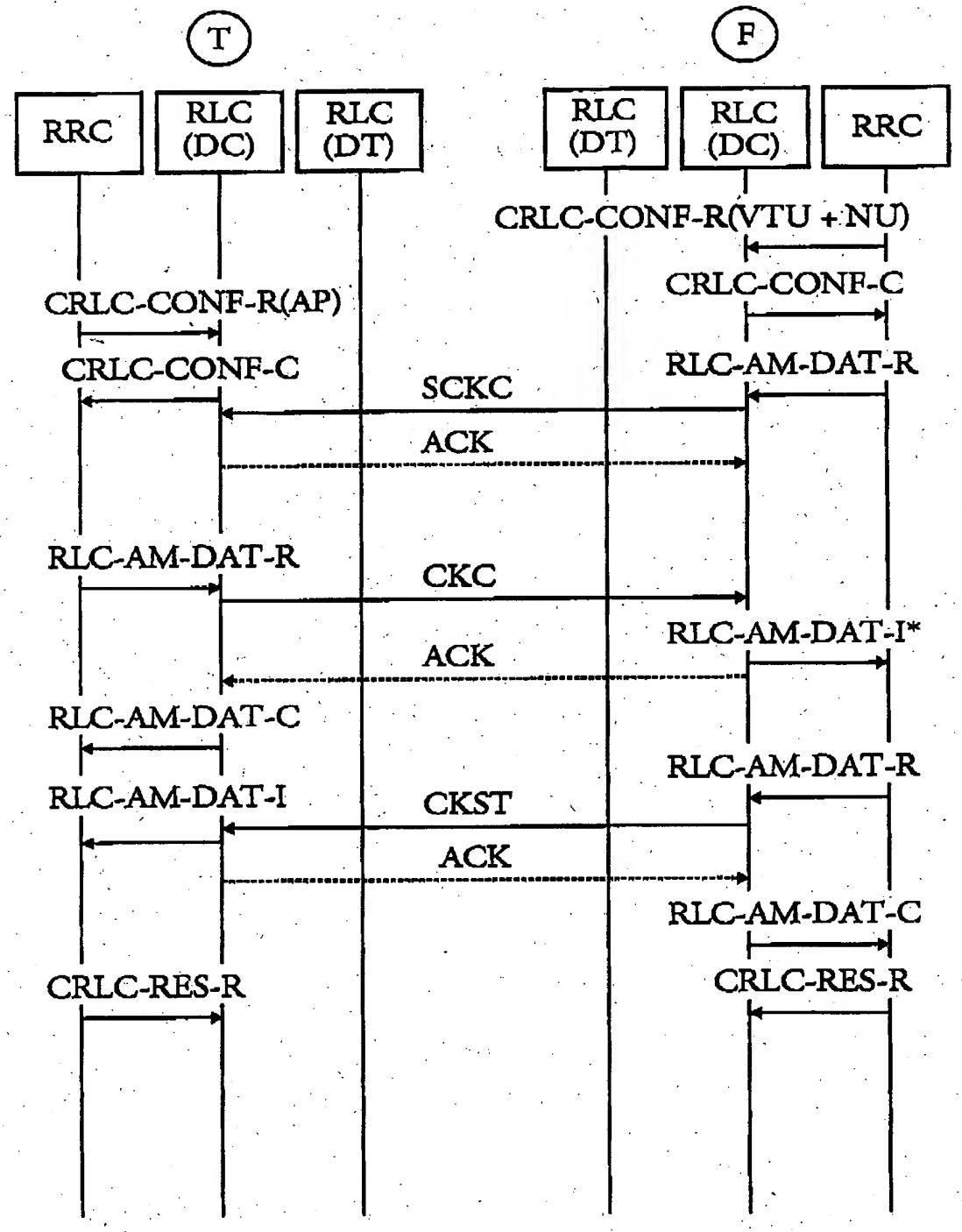

FIG. 5

4-V-PHDE000011

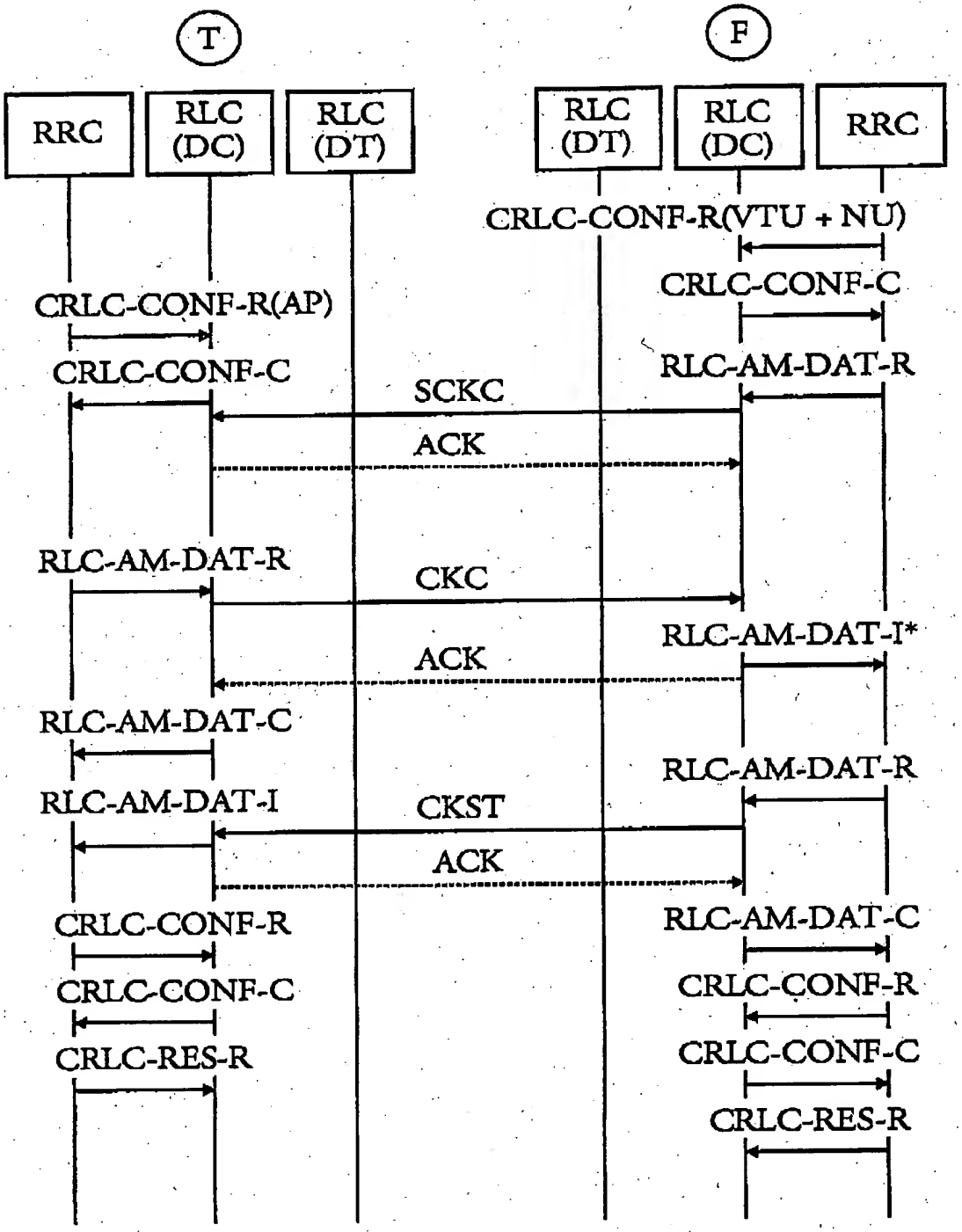

FIG. 6

5-V-PHDE000011